ISACA
Serving IT Governance Professionals
San Francisco Chapter

Infrastructure Vulnerability Assessment

Presented by:

AAA Northern California, Nevada & Utah

Derek Koopowitz – IT Audit Manager
Norm Gutierrez – IT Audit Specialist

Infrastructure Vulnerability Assessment Agenda

- What Is A Vulnerability Assessment?
- Vulnerability Assessment Process
- Business Case For A Vulnerability Assessment
- Footprinting
- Testing Network Security
- Testing Operating System and Web Application Security
- Testing Database Security
- Vulnerability Management
- Q & A

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

What Is A Vulnerability Assessment?

Generally called *Ethical Hacking* or *Network Penetration* testing. Another term used these days is Red Teaming. Essentially we are trying to detect network and system vulnerabilities and to test security by taking an "attacker" like approach in order to gain access. We want to enhance security in our infrastructure and a VA is a great way to accomplish that goal.

What Is A Vulnerability Assessment? (cont'd)

A vulnerability assessment is being proactive. It determines one's susceptibility to an attack before the infrastructure is exploited, and it forces companies to take early corrective action (hopefully). It can show the consequences of an attack to your organization.

Vulnerability Assessment Process

- Impartial assessment – should not be done by IT (fox guarding the hen house)
- Customer consent must be obtained
- Define the scope – general or specific depending on cost/time. Areas to test can be:
  - Internet security (port scanning, password cracking, etc.)
  - Communications security (VM testing, modem testing, etc.)
  - Information security (privacy, etc.)
  - Social engineering
  - Wireless security
  - Physical security (access controls, etc.)

Business Case For A Vulnerability Assessment

- Protect the crown jewels (data)
- Comply with Federal/State laws such as SOX, HIPAA and Privacy
- Comply with vendor requirements such as PCI
- Avoiding unneeded publicity for your company (i.e. TJ Maxx, ChoicePoint)
- Preparing For Potential Infrastructure Breach
- Independent Assessment

Footprinting

Layman's term is reconnaissance. This is the information gathering aspect of the VA – obtain all system and user information to understand the environment. Use this information to execute local and remote attacks. Reduces the risk of being discovered.

Footprinting (cont'd)

Methodology used:

- Publicly available information
  - Company web pages
  - SEC Edgar
  - Search sites (Yahoo, Google, etc.)
  - Usenet
  - Job postings

Footprinting (cont'd)

Methodology used:

- Internet footprinting
  - Whois
  - ARIN
  - Traceroute
  - NSLookup

Footprinting (cont'd)

Methodology used:

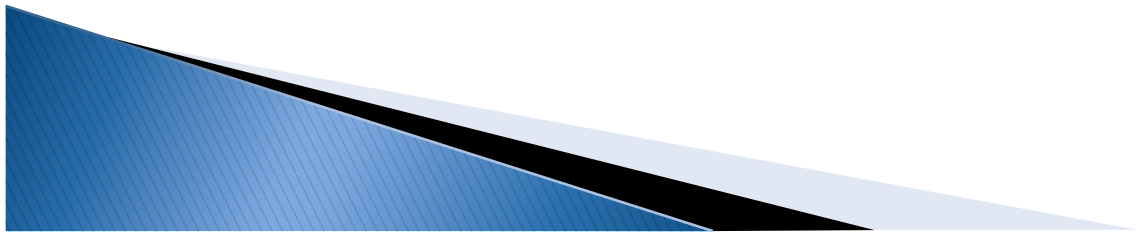
- Scanning
  - Port scanning (ping sweep, etc.)
  - Network scanning (nmap, Superscan, etc.)
  - Vulnerability scanning (Nessus, Satan, etc.)
  - Wardialing (Phonescan, Toneloc, etc.)
  - Banner grabbing

Testing Network Security

- Why test the network
- What is the objective of testing
- Risks associated with not testing
- How to test the network

Testing Operating System and Web Application Security

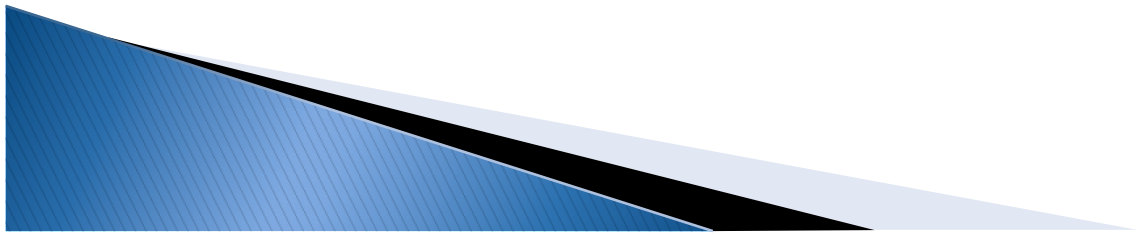
- Why test OS and application security
- What is the objective of testing
- Risks associated with not testing
- How to test the OS and application



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Testing Database Security

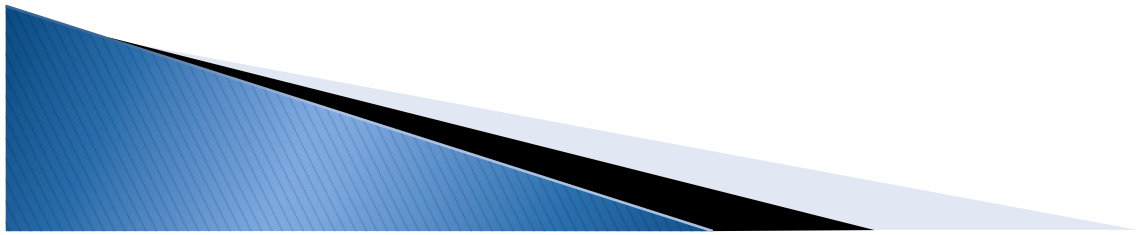
- Why test database security
- What is the objective of testing
- Risks associated with not testing
- How to test database security



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Infrastructure Vulnerability Assessment Computer Networks

- Presentation
  - Protocol Models
  - Communication Components and Devices
  - Infrastructure Attacks
  - Infrastructure Vulnerabilities
  - Passive Attacks
- Demonstration
  - Sniff Passwords Over a Network
  - Sniff Passwords Over a Wireless Network
- Q & A



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Protocol Models

Communication Architecture and Protocols

- ISO's OSI Model
- DARPA's TCP/IP Model

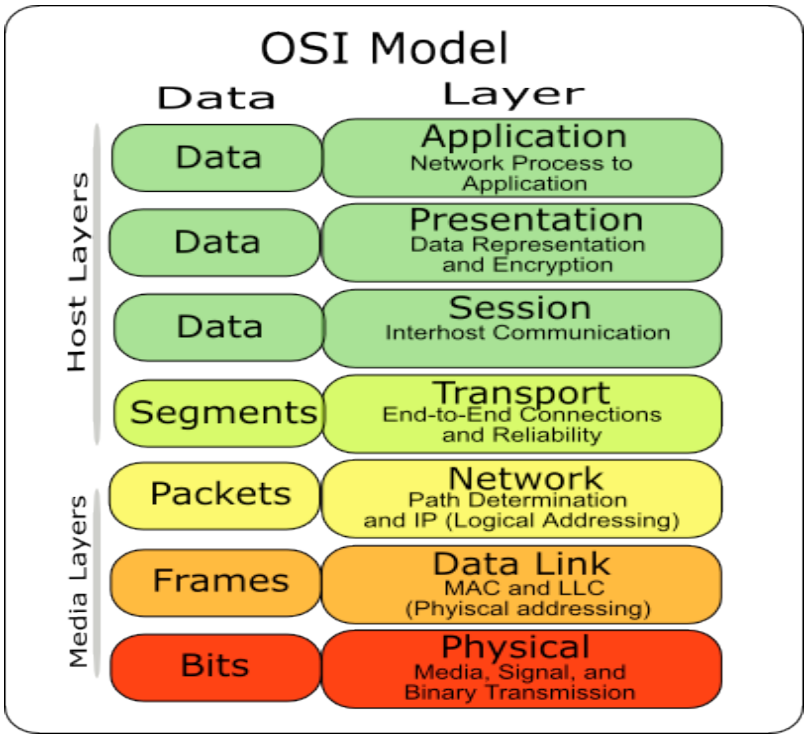
Acronyms

- ISO – International Organization for Standardization
- OSI – Open Systems Interconnection
- DARPA – Defense Advanced Research Projects Agency
- TCP – Transmission Control Protocol
- IP – Internet Protocol

OSI Model

OSI is a computer-communications architecture that uses layering. Each layer performs a related subset of the functions required to communicate with another system. It relies on the next lower layer to perform more primitive functions and to conceal the details of those functions.

Seven Layers Of The ISO/OSI Model



ISACA
Serving IT Governance Professionals
San Francisco Chapter

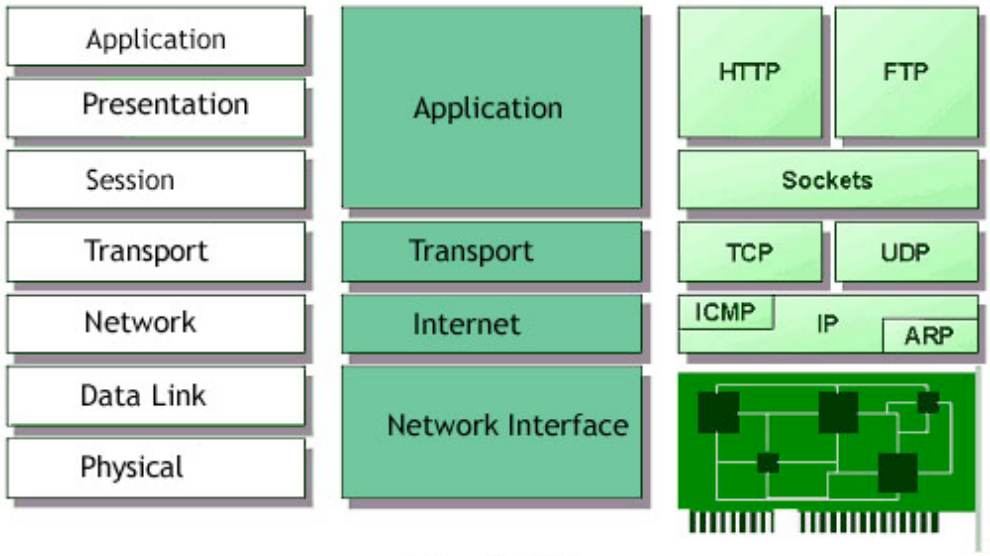
OSI Seven Layers And Function

- Physical – Deals with electrical and mechanical procedures (bits) to establish, maintain, deactivate physical links
- Data Link – Sends blocks (frames) of data across physical link providing flow control and error recovery
- Network – Provides upper layers with independence from data transmission and switching technologies
- Transport – Provides reliable, transparent transfer of data between end points, flow control and error recovery
- Session – Provides controls structure for communication between cooperating applications
- Presentation – Performs generally useful transformations on data to provide a standardized application interface and to provide common communications services; encryption, text, compression, reformatting
- Application – Provides services to users. Defines network applications to perform tasks such as file transfer, e-mail, network management

OSI Relationship With TCP/IP Protocol Suite

- OSI is a reference to protocols, specifically ISO standards, for the interconnection of cooperative computer systems
- TCP/IP is a type of OSI protocol
- When referring to ISO standards, TCP/IP is not an OSI protocol (i.e., TP-0,TP-1)

OSI Layer Mapped To TCP/IP Mapped To Protocols



OSI and TCP/IP

TCP/IP Background

- TCP/IP Protocol Suite resulted from research funded by DARPA
- The protocol suite was designed to foster communication between computers:
  - With diverse hardware architectures
  - To accommodate multiple computer operating systems
  - Using any packet switched network

TCP/IP Background (cont'd)

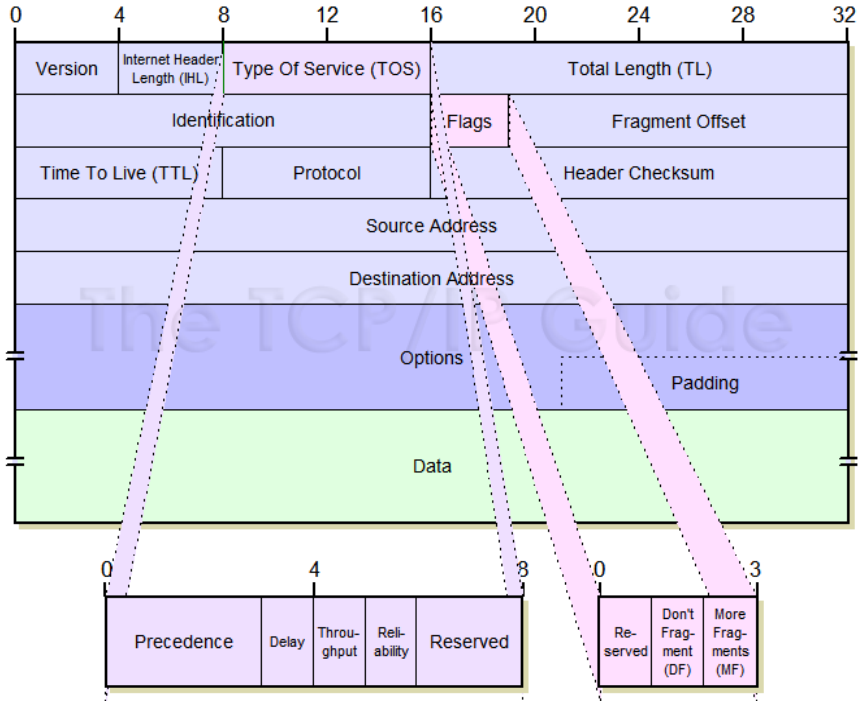
- TCP/IP Protocol Suite Provides Three Conceptual Sets of Internet Services
  - Application Services
  - Reliable Transport Service (TCP)
  - Connectionless Packet Delivery (UDP)

Note: User Datagram Protocol (UDP)

IP Datagram Anatomy

- TCP/IP's Basic Transfer Unit is an **IP Datagram**

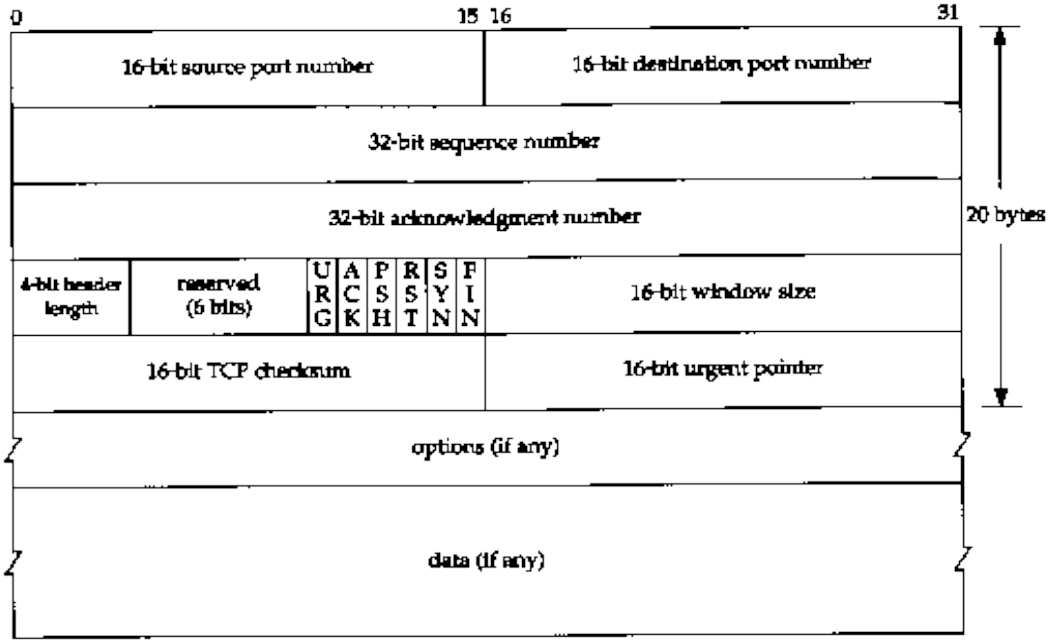
<u>Fields</u>
VER – Version
HLEN – Header Length
Service Type
Length
ID, Flags, and Flags Offset
TTL – Time To Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
IP Options
Padding
Data



TCP Anatomy

TCP Packet Segment Format

- Source Port
- Destination Port
- Sequence Number
- Acknowledgement Number
- HLEN
- Reserved
- Code Bits
- Window
- Checksum
- Urgent Pointer
- Options (IF ANY)
- Padding
- Data

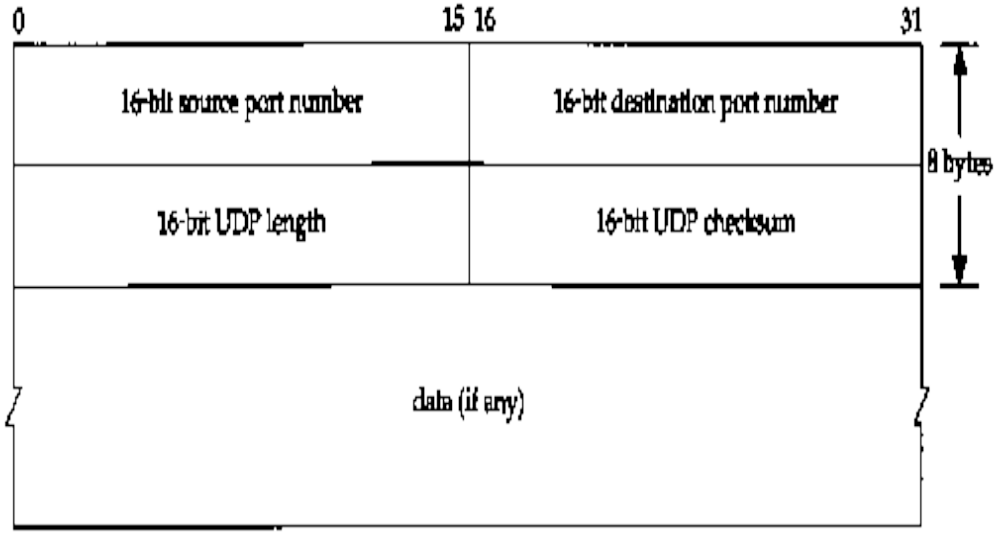


ISACA
Serving IT Governance Professionals
San Francisco Chapter

UDP Anatomy

UDP Packet Segment Format

- Source Port
- Destination Port
- Length
- Checksum
- Data



Communication Components

- Packet – A physical message unit entity that passes through a network sending and receiving data between two computers
  - It usually contains only a few hundred bytes of data
  - Carries identification that enables computers on the network to know whether it is destined for them or how to send it on to its correct destination
- Networks – Packet-Switched Networks

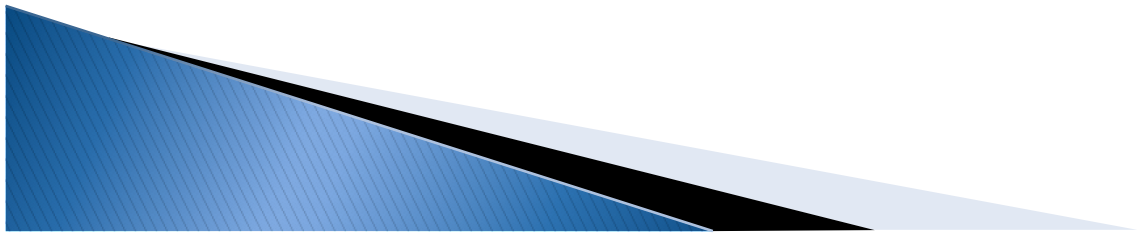
Packet Switched Network Technologies

Some examples are:

- MPLS – *Multiprotocol Layer Switching*
- Ethernet
- X.25
- Frame Relay

Network Devices

- Hubs
- Switches
- Routers
- Firewalls



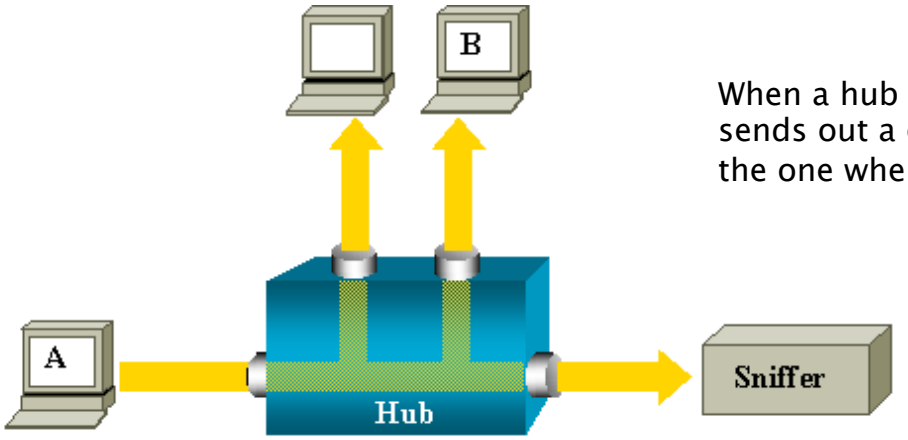
Hubs

- Operates at Layer 1 (Physical) of the OSI model
- Forwards packets by simply broadcasting to every port
- Does not look at address information
- Floods incoming packets to every port
- Each port is the same collision domain
- Each port shares the available bandwidth and hosts must contend for access

Switches

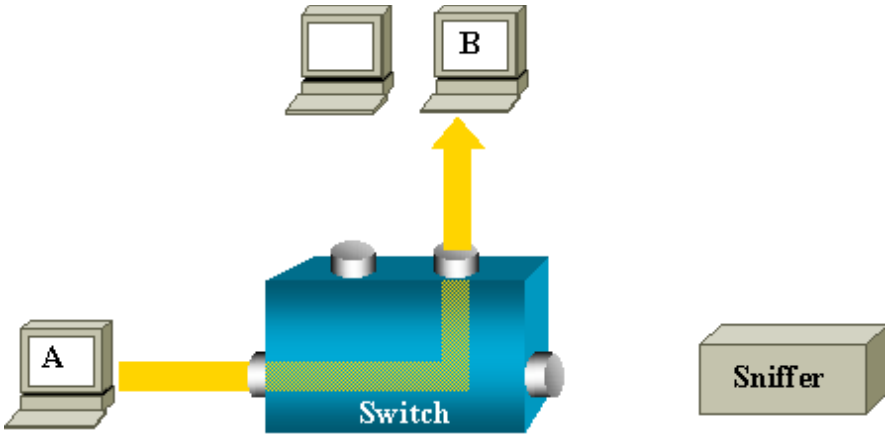
- Operate at Layer 2 (Datalink) protocol
- Switches forward traffic based on destination MAC address
- Ports are not in the same collision domain
- Switches create a private connection between hosts on a network with full access of medium's bandwidth to complete a transaction

Hub vs. Switch – How They Differ



When a hub receives a packet on one port, the hub sends out a copy of that packet on all ports except on the one where the hub received the packet

On a switch, after the host B MAC address is learned, unicast traffic from A to B is only forwarded to the B port. Therefore, a sniffer would not be able to see this traffic.



Routers

- Routers interconnect different technologies spanning various distances and locations (Internet vs. Intranet)
- Operate at Layer 3 (Network) providing routable addressing
  - IP is a Layer 3 Protocol
  - IP addresses contain for 4 octets (i.e. 69.147.114.x)
- Routers forward traffic between IP networks
  - Traffic doesn't flood
  - Router rely on Routing Table

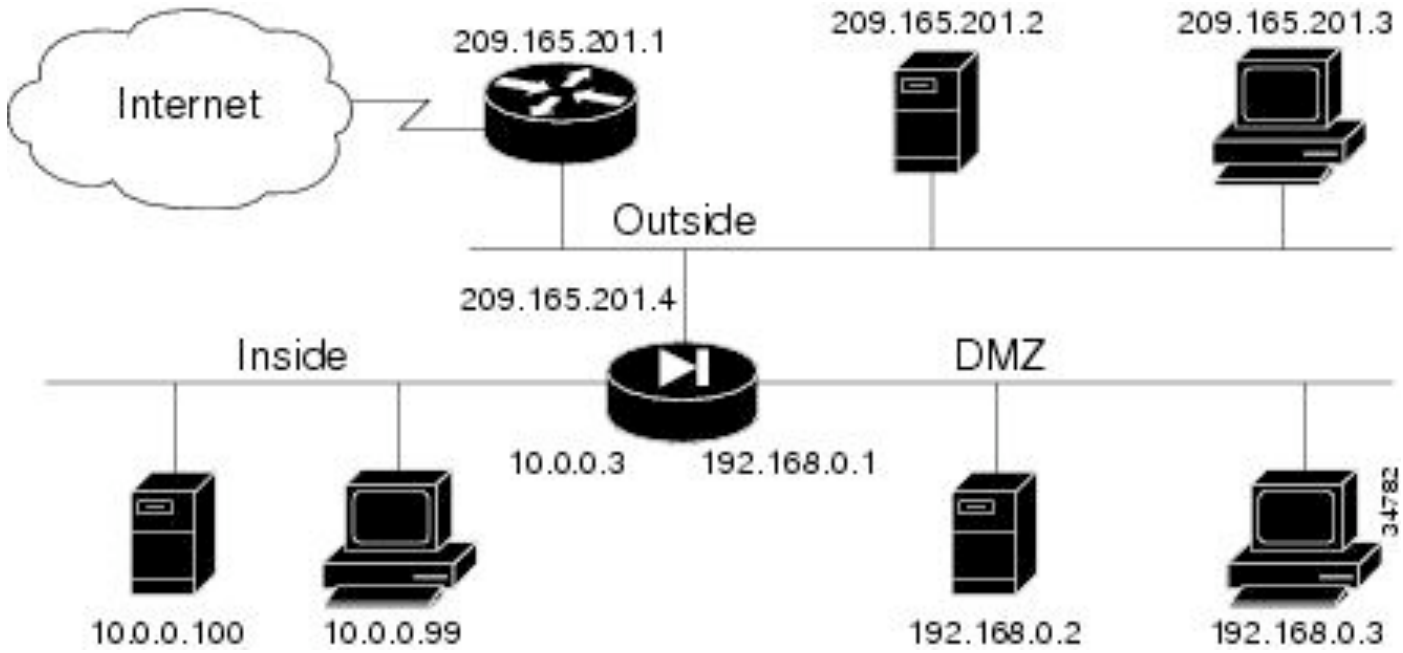
Firewalls

- Operates at Layer 3 (Network). Allows and denies selected IP traffic to and from network segments and/or hosts (i.e. 192.168.5.0/24) (Note: Proxy Servers Operate at Layer 7)

- 1st Generation Packet Filtering Firewall – Acts by inspecting the packets. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source). This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (it stores no information on connection "state").

- 2nd Generation Stateful Firewall – In addition to inspecting packets, the technology maintains records of all connections passing through the device and is able to determine whether a packet is the start of a new connection, or part of an existing connection

Firewall And Router – Network Diagram



Infrastructure Attacks

- **Degradation and Denial of Service (DoS)**
  - Components have finite resources:
    - Bandwidth
    - Processing Power
  - Resources are vulnerable to exhaustion
    - Causing degradation or denial of service
  - Well-engineered infrastructure can resist simple resource attacks
    - With extra capacity for unexpected load
    - By identifying and filter illegitimate traffic

Infrastructure Attacks (cont'd)

- **Bandwidth Exhaustion**
  - Bandwidth attacks overwhelm a target with traffic
    - With or without legitimate payload
  - Infrastructure most vulnerable where traffic is blindly transmitted
    - Routers forward any packet matching routing table
    - Switches flood broadcasts and traffic destined for unlearned addresses
    - Hubs flood everything
  - Packets can be crafted to look completely random
    - Making filtering difficult

Infrastructure Attacks (cont'd)

- **Multiplying Utilization**
  - Some packets cause targets to send responses
    - Multiplies the use of bandwidth
    - Might flood another network
  - Ping floods
    - Network is flooded with ICMP Echo Requests
    - Echo Replies are sent for each request

Infrastructure Attacks (cont'd)

- **Multiplying Utilization** (cont'd)
  - TCP floods
    - TCP suggests end systems respond to all traffic with a connection acknowledgement or reset
    - Bandwidth attacks overwhelm a target with traffic with or without legitimate payload
  - UDP floods
    - Response is not guaranteed by the protocol
    - End servers may respond

Infrastructure Attacks (cont'd)

- **Process Exhaustion**
  - Some Infrastructure components perform significant processing
    - Switches and routers analyze each incoming packet
    - Stateful packet filters maintain state tables
    - Proxies launch new processes or threads for each connection attempt
  - Firewall processing is vulnerable to TCP and UDP floods
    - Even when sufficient bandwidth remains proxy firewalls will answer each request
    - Stateful inspection firewalls allocate system resources

Infrastructure Attacks (cont'd)

- **Inside vs. Outside**
  - Attacks from outside usually affect public services
    - Aimed at the organization's public servers and WAN services
    - Prevents access to and from the Internet
  - Attacks from inside can disrupt internal services
    - Usually from compromised internal systems
    - Prevents access to internal servers and networks
    - Flooding internal networks requires substantial traffic rates

Infrastructure Attacks (cont'd)

- **Distributed DoS**
  - Resource attacks can be initiated from a single source
    - Requires the attacking host have sufficient resources
  - Many resource attacks are controlled by distributed toolsets
    - Installed on previously compromised systems
  - A popular DDos toolkit is TribeFloodNet(TFN)

Infrastructure Attacks (cont'd)

- **Covert Channels**
  - Covert channels transmit data in non-standard ways
    - Place data in non-suspicious packets or header fields
    - Packet header fields are rarely interpreted as information carriers making them ideal for use as covert channels
      - ✓ IP fragment ID
      - ✓ TCP sequence number
      - ✓ Usually from compromised internal systems
  - Packets can be bounced off intermediate systems
    - Useful if firewall limits inbound traffic to trusted sites
  - Proxy and NAT-based firewalls limit the effectiveness of covert channels
    - Because they rewrite packet headers

Infrastructure Attacks (cont'd)

- **Device Configuration Vulnerabilities**
  - Many infrastructure components must be configured by administrators
    - Switches, routers, and firewalls
  - Remote administration is convenient and sometimes essential
  - Administration protocols can introduce configuration vulnerabilities
    - Telnet and HTTP
    - Simple Network Management Protocol (SNMP)
    - Dynamic routing protocols such as RIP, OSPF, and BGP

Infrastructure Attacks (cont'd)

- **SNMP Vulnerabilities**
  - SNMP is the de facto standard for remotely monitoring devices
    - Can also be used to configure them
  - SNMP v1 uses inherently vulnerable techniques
    - Implemented over UDP
    - Transmits passwords unencrypted
    - Widespread use of default passwords: public and private
  - Most implementations are vulnerable to attack
    - By sending misformatted queries
    - Attack devices can stop functioning
  - Later versions of SNMP mitigate these risks
    - Better authentication
    - Encryption

Infrastructure Attacks (cont'd)

- **Telnet and HTTP Vulnerabilities**
  - Default security settings are often inadequate
    - Factory passwords
    - Unrestricted access
  - Passwords are transmitted in the clear
    - Sometimes transiting production networks
    - We'll explore eavesdropping on passwords
  - Routine security procedures can mitigate the risk
    - Restrict access to the minimum number of addresses
    - Keep administration traffic on protected segments
    - Regularly change passwords and use encryption

Infrastructure Attacks (cont'd)

- **Routing Protocol Vulnerabilities**
  - Routers can be attacked by transmitting spoofed routing information
    - Some routing protocols have poor security mechanisms
  - RIP routing information is broadcast
    - Any host on the router's subnet can inject routes
  - OSPF routing information is multicast
    - Any host on the router's subnet can inject routes
  - BGP routing information is unicast
    - Hardest to spoof

Passive Attacks

- **Benefits of Sniffing**
  - Sniffers are used to diagnose network problems
    - Technicians view actual packet exchanges for troubleshooting
  - Monitoring traffic as part of routine network management
    - Bandwidth use, packet sizes, protocol distribution, etc.
  - IDS relies on sniffing network traffic
    - Signatures match on packet payload

Passive Attacks (cont'd)

- **Dangers of Sniffing**
  - Many application protocols transmit payload unencrypted
    - E-mail and instant messaging
    - Telnet, FTP, and Web servers
    - Authentication exchanges sent "in the clear"
  - Attackers often install sniffers on compromised hosts
    - Save decoded packets for later retrieval
    - User names and passwords can be easily discovered

Passive Attacks (cont'd)

Sniffing Hubs and Switches

- Hubs make promiscuous sniffing very easy
  - All traffic transiting a hub is repeated out all ports
  - A sniffer connected to any hub port sees all traffic on the hub
- Switches are not "sniffer-friendly"
  - Unicast traffic transiting a switch is forwarded to a single port
    - Based on the destination MAC address
  - Each port is a separate collision domain
  - Sniffer connected to a switch port sees only that port's traffic
- Common belief: Switches prevent sniffing other hosts
  - Not true!
- Two techniques for sniffing a switched environment
  - MAC flood attacks the switch
  - ARP poisoning attacks

Passive Attacks (cont'd)

- **Remote Access**
  - Many organizations provide facilities for remote access to their network
    - Dial-up modem banks
    - Wireless access points
    - Virtual Private Network (VPN)
  - Often these facilities terminate behind a security boundary
    - Bypass firewall systems and IDS
    - Allow an outside system to appear as an inside system
  - Discovering and exploiting remote access can provide inside access

Passive Attacks (cont'd)

- **Wireless Networking**
  - Wireless networking installations
    - Following the IEEE 802.11 Series of standards
  - Wireless networks can be configured in two ways
    - Peer-to-Peer
    - Wireless LANS (WLAN)

Passive Attacks (cont'd)

- **Wireless Networking (cont'd)**
  - Insecure WAPs result in critical exposure of internal networks
    - WLANs behind firewall provides a backdoor to the inside network
    - Traffic can be sniffed without physical inside access

Summary

- When auditing an application, system or environment, test the network segment it resides on
- Controls and security are only as good as the network
- Minimize attack surface by segmenting networks and forcing only authorized physical access to network

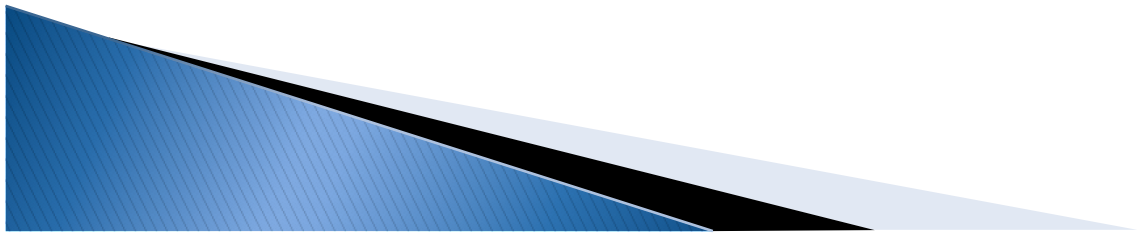
Sniff Traffic Over A Network – Demo

- Create a "mirror" image of data going through a network device
- Use a hub for fanning out data to a read-only analyzer
- Use an open-source network analysis tool running over Linux or Windows such as Snort or Ethereal protocol analyzer
- View data and passwords in clear text

Analyze The Security Of A Wireless Network – Demo

- Identify Wireless Access Points using an Open Source Tool (i.e. Kismet)
- Compromise WLAN using a WEP Cracking Tool (i.e. Airsnort)
- Scan WLAN for vulnerable nodes
- Compromise a multi-homed node with both WLAN and LAN access
- Compromise a second node that resides on a separate LAN (optional)

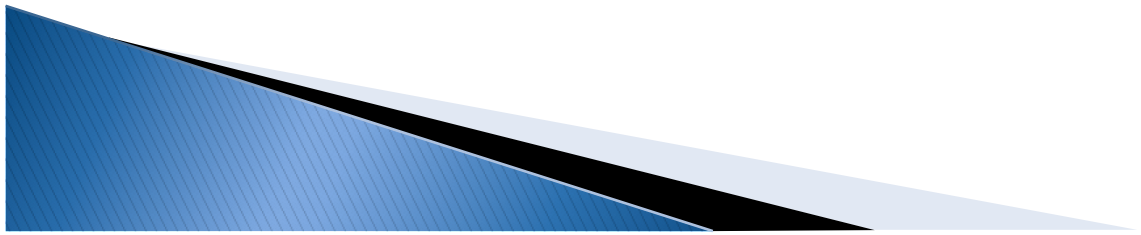
Q & A



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Infrastructure Vulnerability Assessment Operating Systems And Web Applications

- Presentation
  - OS Shared Services Dependencies
  - Common System and Application Vulnerabilities
- Demonstration
  - Testing System Security
  - Testing Password Security
  - Testing Web Server Security
  - Windows Null Session Vulnerability
- Q & A



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

OS Shared Services Dependencies

- Components supported by operating systems
  - Systems
    - DNS
    - IIS
    - Active Directory
    - E-Mail
    - Web

Common System And Application Vulnerabilities

- Introduction of System Vulnerabilities
  - Incorrect configurations
  - Poor programming producing software bugs
  - Default settings applied
  - Default passwords
  - Windows Null Session vulnerability

Incorrect Configurations

- Incorrect system configuration lead to system vulnerabilities
- Antivirus signatures out of date leave systems exposed to Trojans and other malware
- During period of outdated antivirus signature definition
- Potential resultant exploit impacting an infected system:
- *Infected system sending company data outbound*

Incorrect Configurations (cont'd)

- Outbound traffic on port 80 and/or 443 unrestricted
  - Outbound traffic sourced from a compromised system – corporate data egress company firewall via port 80 or 443 unnoticed (keystroke loggers, Trojans)
- Un-patched Web server Operating Systems
- Incorrectly configured Web server applications (IIS, Apache)
- Sound threat and vulnerability management program is essential
- Ensure workstations are patched and anti-virus / spyware definitions are up to date

Poor Programming Producing Software Bugs

- Unsecured coding practices
- Lack of secure coding education and training and necessary security analysis tools to test for insecurely written code instances
- Unsecured web applications residing on public facing web sites
- Potential resultant Identity Theft exploits below:
  - *SQL Injection*
  - *Cross Site Scripting*

Default Settings Applied

- Unnecessary services i.e. Telnet, FTP, SMTP turned on by default for ease of use and immediate functionality availability
- Lack of configuration management standards to secure the OS after deployment
- During system build process and/or environment change
- Malware potentially exploiting vulnerable systems with unnecessary services running

Default Passwords

- Obtain user account credentials with administrator or root privileges
- Passwords are generally stored and transmitted in an encrypted form called a *hash*
- Password cracking employs captured password hashes
- Passwords hashes can be intercepted when they are transmitted across the network (using a network sniffer) or they can be retrieved from the targeted system

Default Passwords (cont'd)

- The latter generally requires administrative or "root" access on the target system
- User configuration error
- Vendor supplied passwords are not changed. Absence of system specific configuration management standards – go to www.defaultpasswords.com for more information.
- During system build process or environment change

Windows Null Session Vulnerability

- Windows OS default behavior (IPC$)
- Windows administrative shares use IPC to communicate
- When LAN Manager authentication is permitted in a Windows environment

Testing System Security – Demo

- Scan systems for vulnerabilities
  - Perform Nessus and/or MBSA scan of *W2K Server* – displaying un-patched systems
  - Install keystroke logger and/or Trojan on Workstation
  - Show where keystroke logger is sending data via outbound e-mail from compromised workstation

Testing Password Security – Demo

- Obtain a password hash file from a vulnerable system
- Show tools to crack password hashes
  - Use tools to identify and exploit weak passwords using password cracking tools

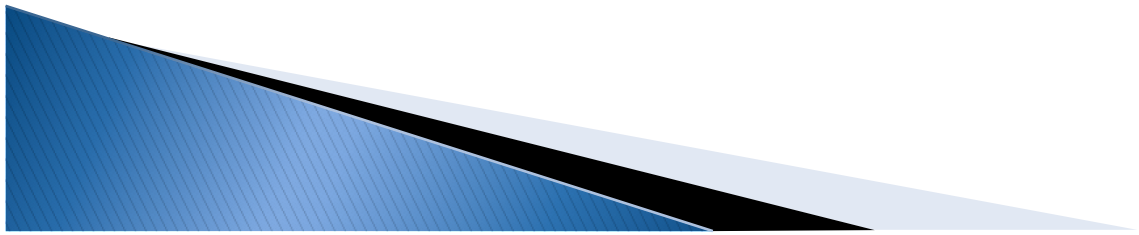
Testing Web Server Security – Demo

- Analyze the security of a web server
  - Use tools to identify and exploit a web application to elicit an improper response from the site – that could potentially lead to disclosure of private information or phishing attacks

Testing Web Server Security – Demo

- Show how null session is exploited

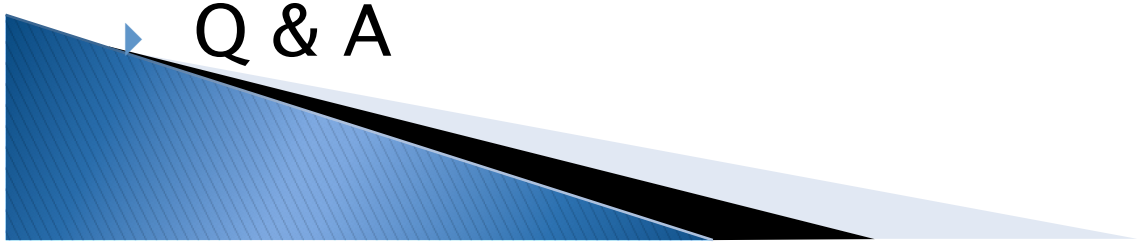
Q & A



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Infrastructure Vulnerability Assessment Relational Database Systems

- Presentation
  - Relational Database Overview
  - SQL
  - Oracle Configuration Vulnerabilities
  - Footprinting Databases
  - Enumerating an Oracle Server
  - Attacking the TNS Listener
  - Mitigating Oracle Vulnerabilities
- Demonstration
  - Enumerate and Compromise an Oracle Database
- Q & A



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Relational Database Overview

Examples of Relational Database Products

- Oracle
- Microsoft SQL Server
- DB2
- MySQL
- PostgreSQL
- Microsoft Access

Relational Database Overview (cont'd)

- A database management system (DBMS) is the software which controls the storage, retrieval, deletion, security, and integrity of data within a database
- An RDBMS is a DBMS which manages a relational database
- A relational database stores data in tables
- Tables are organized into columns, and each column stores one type of data (i.e. integer, real number, character strings, date)
- The data for a single "instance" of a table is stored as a row

Relational Database Overview (cont'd)

- For example, the Customer table would have columns such as CustomerNumber, FirstName, and Lastname, and a row within that table would be something like {1701, "John", "Doe"}
- Tables typically have keys, one or more columns that uniquely identify a row within the table, in the case of the Customer table the key would be CustomerNumber
- To improve access time to a data table you define an index on the table. An index provides a quick way to look up data based on one or more columns in the table, just like the index of a book enables you to find specific information quickly

Relational Database Overview (cont'd)

- The most common use of RDBMS's is to implement simple CRUD – Create, Read, Update, and Delete – functionality
- For example an application could create a new transaction and insert it into your database
- It could read an existing transaction, work with the data, and then update the database with the new information
- It could also choose to delete an existing transaction, perhaps because the customer has cancelled it

Relational Database Overview (cont'd)

- The vast majority of your interaction with an RDBMS will likely be to implement basic CRUD functionality
- The easiest way to manipulate a relational database is to submit Structured Query Language (SQL) statements to it
- SQL retrieves and manages data stored in a relational database system

SQL

- Auditor's can quickly review controls using SQL statements
- Scripts can be used to execute numerous key SQL statements that provide valuable information
- Common criticisms of SQL include a perceived lack of cross-platform portability between vendors, inappropriate handling of missing data (i.e. null fields), a complex three-valued logic system, and its complex and occasionally ambiguous language grammar and semantics

Oracle Configuration Vulnerabilities

- Oracle has default userid's and passwords
  - Default accounts if enabled or unchanged could result in gaining DBA privileges
- Examples of Oracle Default accounts and passwords
  - SYS = CHANGE_ON_INSTALL
  - DBSNMP = DBSNMP
  - CTXSYS = CTXSYS
  - MDSYS = MDSYS
  - OUTLN = OUTLN

Oracle Configuration Vulnerabilities (cont'd)

- If operating system controls are weak the ability to connect and gain DBA privileges exist
- Oracle inserts an OS user account into a member group (i.e., DBA_ORG) which allows that user to gain DBA access

SQL Server Vulnerabilities

- Blank SA password
- Buffer overflow can occur with an overly long request for SQL servers is sent to UDP port 1434
- Direct exploit attacks using a tool such as Metasploit
- SQL injection
- Blind SQL injection
- Extended stored procedures contain buffer overflows

Footprinting Databases

- Utilize a port scanner to look for common ports used by database servers
- Examples of default ports are:
  - 1433/1434 – Microsoft SQL
  - 1521 – Oracle
  - 4100 – Sybase

Enumerating An Oracle Server

- Determine an Oracle version number by connecting to a TNS (Transparent Network Substrate) Listener Service
  - Each Oracle version has known vulnerabilities
- Identify Database Instances
  - In order to access data in the database you need to have an instance name

Attacking The TNS Listener

- A TNS Listener without an assigned password allows for:
  - Enumeration which can lead to compromise
  - A remote user to execute a command which could fill up a log file on the local file system until system halts

Mitigating Oracle/SQL Server Vulnerabilities

- Set a TNS Listener Password
- Set an SA Password (SQL Server)
- Turn on Admin Restrictions
- Turn off External Procedures
- Turn off XML Database
- Encrypt Network Traffic
- Lock and Expire Unused Accounts
- Change Default Passwords

Mitigating Oracle/SQL Server Vulnerabilities (cont'd)

- Define and Enforce a Good Password Policy
  - Password Length
  - Password Expiration Date
  - Password History
- Roles
  - Permissions should be granted on the principle of least privilege
- Disable Remote Authentication
- Enable Account Lockout
- Limit the number of accounts that are assigned a DBA role

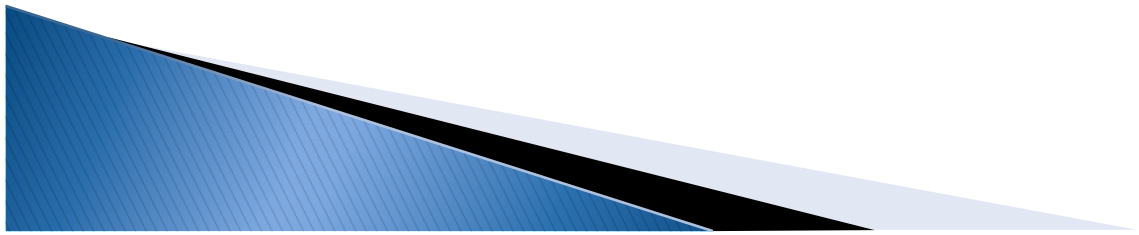
Mitigating Oracle/SQL Server Vulnerabilities (cont'd)

- Enable Auditing
- Enable Data Dictionary Protection
- Enable Database Link Login Encryption
- Create Triggers
- Conduct audits to ensure security posture is acceptable
- Patch, patch, patch…

Enumerate Oracle – Demo

- Scan for Open Ports
- Connect to TNS
- View Database Instance
- Connect to instance via SQL
- Exploit Default Password Vulnerability
- Download Password Hash File
- Use a program like CAIN AND ABEL to crack passwords

Q & A



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Vulnerability Management

What is a vulnerability management process?

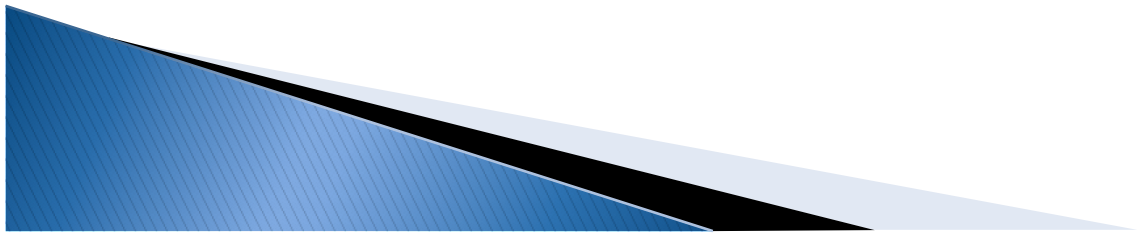
- What systems do we have?
  - Current inventory of systems (hardware and software)
- Identify vulnerabilities and prioritize based on risk
  - Gather information which focuses on the vulnerabilities affecting your systems
  - Evaluate the actual risks to your organizations security
- Fixing the vulnerabilities
  - Plan for a response (i.e. patching and fixing systems)
- Evaluate the end result
  - Trends in vulnerabilities
  - Systemic errors

Vulnerability Management (cont'd)

Vulnerability management isn't…

- Just scanning – requires acting on the results of the scans
- Just patching – requires tweaking configurations as well
- Just a technical solution – involves policy and process changes
- Just a local issue – look at the big picture

Q & A



ISACA®
Serving IT Governance Professionals
San Francisco Chapter